

SECURE VOTING SYSTEM

INCORPORATION BY REFERENCE TO ANY PRIORITY APPLICATIONS

[0001] Any and all applications for which a foreign or domestic priority claim is identified in the Application Data Sheet as filed with the present application are hereby incorporated by reference under 37 CFR 1.57. This application claims the benefit of priority to U.S. Provisional application Nos. 62/803,373 and 62/803,296, the entire contents of which are hereby incorporated by reference.

BACKGROUND

Field

[0002] This development relates to a voting system that also incorporates the use of cryptographic elements, such as blockchains, as are used with cryptographic currencies, to track and secure the vote by mail system.

Description of the Related Art

[0003] Voters generally wish to be able to vote for elected officials or on other issues in a manner that is convenient and secure. Further, those holding elections wish to be able to ensure that election results have not been tampered with and that the results actually correspond to the votes that were cast. In some embodiments, a blockchain allows the tracking of the various types of necessary data in a way that is secure and allows others to easily confirm that data has not been altered.

SUMMARY

[0004] In one aspect described herein, a voting system comprises a blockchain access layer configured to: receive input from a user operated mobile computing device, the input comprising a computer readable code scanned from a physical ballot, ballot selections, and an electronic signature; and receive input from an election official system, the input comprising a ballot and an election identifier; a first database in communication with the block chain access layer, the first database configured to receive and store the ballot selections and the electronic signature from the blockchain access layer; a second database in communication with the block chain access layer, the second database configured to: receive a vote identification from the blockchain access layer, the vote identification generated by the blockchain access layer in response to receive the ballot selections and electronic signature from the mobile computing device; store a first pointer to a location of the ballot selections in the first database; and store a second pointer to a location of the electronic signature in the first database; and a blockchain database configured to receive the vote identification from the second database and to receive the ballot selections from the blockchain access layer, wherein the block chain database receives the vote identification and the ballot selections when the block chain access layer receives an electronic signature confirmation from the election official system.

[0005] In some embodiments, the ballot selections and the electronic signatures are stored in separate structures in the first database.

[0006] In some embodiments, the first database has no referential data associating the ballot selections with the electronic signatures stored in the separate structures in the first database.

[0007] In some embodiments, the vote identification is a random alphanumeric string for tracking the instance of a vote.

[0008] In some embodiments, the electronic signature is an object bitmap created within a voting application on the user operated mobile computing device.

[0009] In some embodiments, the election identifier identifies a particular election.

[0010] In some embodiments, the blockchain access layer is further configured to receive a voter identification from the user operated mobile computing device, the voter identification identifying a unique user registered with the election official system.

[0011] In some embodiments, the system further comprises a verification contract database, and wherein the blockchain access layer comprises a verification service module, wherein the verification service module is configured generate a hash of the ballot selections and the electronic signature received in the blockchain access layer, and to send the hash of the ballot selections and the electronic signature to the verification contract database.

[0012] In some embodiments, the blockchain access layer is further configured to send the hash of the ballot selections and the electronic signature to the user operated mobile computing device or to the election official system.

[0013] In some embodiments, the computer readable code includes at least one of a ballot identifier, an election identifier, and a voter identifier, and wherein the blockchain access layer authorizes the mobile computing device access to an electronic ballot based on the ballot identifier, election identifier, or the voter identifier.

[0014] In another aspect, a voting method comprises receiving, in a blockchain access layer, input from a user operated mobile computing device, the input comprising a computer readable code scanned from a physical ballot, ballot selections, and an electronic signature; receiving input from an election official system, the input comprising a ballot and an election identifier; receiving, in a first database, the ballot selections and the electronic signature from the blockchain access layer; receiving, in a second database, a vote identification from the blockchain access layer, the vote identification generated by the blockchain access layer in response to receiving the ballot selections and electronic signature from the mobile computing device; storing, in the second database, a first pointer pointing to a location of the ballot selections in the first database; storing, in the second database, a second pointer pointing to a location of the electronic signature in the first database; and receiving, from the election official system, confirmation of the electronic signature; transmitting, to a blockchain database, the vote identification from the second database and the ballot selections corresponding to the vote identification based on the first pointer; and storing, in the blockchain database, the ballot selections.

[0015] In some embodiments, storing the ballot selections and the electronic signatures in the first database comprises storing the ballot selections and the electronic signature in separate structures in the first database.